September 4, 2008 - CMU Software Engineering Institute Recognized by Congressmen Murtha, Doyle and Altmire

CERT Computer Forensics Team at Carnegie Mellon Software Engineering Institute Recognized by Congressmen Murtha, Doyle and Altmire

Pittsburgh, PA, September 4, 2008 &ndash; The recent U.S. Department of Justice indictment of 11 individuals responsible for the largest identity theft case in history was possible in part to the efforts of the CERT® Program at Carnegie Mellon University&rsquo;s Software Engineering Institute (SEI). U.S. House of Representatives John Murtha , Mike Doyle, and Jason Altmire recognized the program&rsquo;s efforts today during a visit to the university in which the SEI, Carnegie CyLab, and School of Computer Science programs showcased some of the university&rsquo;s latest research and technology initiatives.

CERT&rsquo;s computer forensics team provided support to the U.S. Secret Service (USSS) &ndash; through training, custom-designed forensics tools, and assistance with its electronic evidence acquisition strategy &ndash; during its investigation of the group subsequently indicted for stealing over 40 million credit and debit card numbers of customers shopping at major retailers outlets.

&ldquo;CERT&rsquo;s role in this landmark case underscores its importance in computer security over the past 20 years,&rdquo; says Murtha. &ldquo;The SEI and its relationships with government agencies like the Department of Defense and the Department of Homeland Security have allowed for the successful development of forensics tools to be used by law enforcement agencies and other government sectors.&rdquo;

The USSS electronic crimes task force received computer forensics training through the CERT Virtual Training Environment (VTE), a blend of classroom instruction and self-paced online training in information assurance, computer security, and computer forensics. VTE allows users to access high quality training material through a web browser. The computer forensics training area gives users access to a secured training lab that includes specialized tools developed by CERT to cover gap areas not addressed by commercial tools.

Next, the USSS adopted CERT&rsquo;s Clustered-Computing Analysis Platform, or C-CAP. C-CAP is a state-of-the-art forensics analysis environment that assists commercial and government organizations in identifying the next wave of security challenges when an incident occurs. C-CAP allows organizations to process large amounts of data typically located on networks to examine systems, crack passwords, and analyze network data.

&ldquo;Computer technology and the internet enrich our lives and promote economic growth, they have also made our lives and our economy more vulnerable to hackers and criminals,&rdquo; Congressman Doyle said. &ldquo;Fortunately, we&rsquo;ve got some smart people at Carnegie Mellon working to keep one step ahead of these threats and to help law enforcement agencies like the Secret Service and the FBI track them down and put them in prison. I have worked in Washington with my colleagues from Pennsylvania&rsquo;s Congressional delegation to make certain that the proper federal agencies are aware of the remarkable resources available at Pittsburgh&rsquo;s research universities and to make certain that the federal government makes important investments in local research efforts that will benefit our nation.&rdquo;

Congressman Altmire stated that today&rsquo;s announcement and demonstration of CERT&rsquo;s computer forensics technology is another example of why Carnegie Mellon is such an important asset to western Pennsylvania &ldquo;The university&rsquo;s contribution to the efforts of law enforcement to protect the financial security and personal information of consumers across the country is impressive and will serve to build on its reputation of being on the cutting edge of research and technology,&rdquo; said Altmire.

Murtha also highlighted the current collaborative efforts underway at the Johnstown, Pa.-based National Drug Intelligence Center (NDIC). NDIC is currently working with CERT to transition C-CAP into their environment based on the success and rapid adoption of the technologies by the Secret Service.

Rich Nolan, technical lead for CERT&rsquo;s computer forensics team says that one of the hardest parts about a forensics investigation is finding out where to start. &ldquo;Digital forensics investigators face challenges in getting the evidence they need as encryption and other counter-measures become more common,&rdquo; explains Nolan. &ldquo;We are providing operational support to the Secret Service, to high-profile intrusion and identity-theft investigations and other general computer crimes to help them identify the best place to start.&rdquo;

The mini showcase of technologies from Carnegie Mellon included a demonstration of advances in biometric security devices, applications of mobile technology for persons with disabilities and the application of video game technology for children to foster cardiovascular exercise.

For more information about VTE, C-CAP and other efforts underway at CERT, please visit the CERT website at www.cert.org. Information about Carnegie Mellon and its research initiatives can be found at www.cmu.edu.

About the Carnegie Mellon Software Engineering Institute

The Software Engineering Institute (SEI) is a U.S. Department of Defense federally funded research and development center operated by Carnegie Mellon University. The SEI helps organizations make measured improvements in their software engineering capabilities by providing technical leadership to advance the practice of software engineering. For more information, visit the SEI website at http://www.sei.cmu.edu.